UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/733,537	12/07/2000	Philip R. Graham	2705-697	1789

20575 7590 12/26/2007

MARGER JOHNSON & MCCOLLOM, P.C.
210 SW MORRISON STREET, SUITE 400
PORTLAND, OR 97204

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
12/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	09/733,537	GRAHAM, PHILIP R.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *7,11-13,17,21-27,30 and 31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7,11-13,17,21-27,30 and 31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 7, 11-13, 17, 21-27, 30 and 31 are pending in this office action, claims 8-10, 18, 19, 28, and 29 are canceled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 11, 2007, has been entered.

3. Applicant's arguments, filed October 11, 2007, are moot in view of the new ground of rejection.

Rejections

4. The text of those sections of Title 35, U.S. Code not included in this office action can be found in a prior Office action.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 7, 11-13, 17, 21-27, 30 and 31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Regarding claims 7, 17, 21, 27, 30, and 31, the trademark names "MP3," "MPEG," and "Word" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP 2173.05(d). Claims 11-13, 22-26 are dependent upon claims 7 and 21 and therefore inherit their deficiencies.

Claim Rejections - 35 USC § 103

8. Claims 7, 11, 12, 21, 22, 24, 25, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6,389,532) in view of Hale et al. (U.S. Patent No. 6,732,180).

Regarding claims 7 and 30, Gupta et al. teaches a restricted data format method/system for a network infrastructure copy protection system, comprising:

- Receiving a digital content file for transmission across a distributed computer network (fig. 7, ref. num 702);
- Examining data comprising the content file, the examining performed within the distributed computer network (fig. 7, ref. num 704 and 706).

Gupta et al. does not teach to the examining is to determine whether the content file comprises a restricted data format, transmitting the content file when the data

comprising the content file does not include the restricted data format, and blocking the transmission of the content file when the data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

Hale et al. teaches examining the content file to determine whether the content file comprises a restricted data format (col. 3, lines 9-12), transmitting the content file when the data comprising the content file does not include the restricted data format and blocking the transmission of the content file when the data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, **wherein the restricted data format is an MP3 data format, a MPEG video data format, and a Word document format** (col. 3, lines 12-17), wherein the blocking is effected prior to a transmission of the content file to a receiver (col. 3, lines 12-17).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine examining a content file for restricted data formats, and transmitting the content file if not restricted data formats exist and blocking transmitting of restricted data formats do exist, as taught by Hale et al., to the restricted data format method/system of Gupta et al. It would have been obvious for such modifications because preventing multimedia from being streamed protects copyrights (see col. 3, lines 1-9 of Hale et al.).

Regarding claims 11 and 24, the combination of Gupta et al. in view of Hale et al. teaches the distributed computer network is the Internet (see col. 5, lines 15-20 of Gupta et al.).

Regarding claims 12 and 25, the combination of Gupta et al. in view of Hale et al. teaches the examining is performed by a plurality of routers within the distributed computer network (see fig. 1, ref. num 104 of Gupta et al.).

Regarding claim 21, Gupta et al. teaches a network device comprising:

- A bus (fig. 2a, ref. num 237);
- Computer readable memory units connected to said bus (col. 2a, ref. num 204);
- One or more processors coupled to said bus, said computer readable memory units for executing a digital signature method for a network infrastructure copy protection system (fig. 2a, ref. num 202), comprising:
    - Applying a digital signature to a digital content file (fig. 3, ref. num 310);
    - Examining the **digital** content file to determine whether the **digital** content file includes the digital signature, wherein the examining is performed within a distributed computer network (col. 3, lines 50-54);
    - Transmitting the **digital** content file when the **digital** content file includes the digital signature (col. 4, lines 7-11);

- Blocking transmission of the **digital** content file when the **digital** content file does not include the digital signature to prevent unauthorized downloading of copyrighted material (col. 4, lines 12 and 13).

Gupta et al. does not teach blocking transmission of the **digital** content file when the data comprising the **digital** content file is a restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the **digital** content file to a receiver.

Hale et al. teaches blocking transmission of the **digital** content file when the data comprising the **digital** content file is a restricted data format to prevent unauthorized downloading of copyrighted material**, wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format**, wherein the blocking is effected prior to a transmission of the **digital** content file to a receiver (col. 3, line 9-17).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine blocking transmission of the content file if the content file contains a restricted data format, as taught by Hale et al., to the network device of Gupta et al. It would have been obvious for such modifications because preventing multimedia from being streamed protects copyrights (see col. 3, lines 1-9 of Hale et al.).

Regarding claim 22, the combination of Gupta et al. in view of Hale et al. teaches wherein the digital signature is configured to identify the sender of the digital content file (see col. 3, lines 44-46 of Gupta et al.).

Claims 13, 17, 23, 26, 27, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (USPN '532) in view of Hale et al. (USPN '180), and further in view of Gibbs et al. (U.S. Patent No. 6,085,321).

Regarding claims 17, 27, and 31, Gupta et al. teaches a network infrastructure/device/system protection method for detecting and denying transmission of restricted data formats, comprising:

- One or more network interfaces (fig. 2a, ref. num 237);
- Computer readable memory units connected to a bus (fig. 2a, ref. num 204);
- One or more processors coupled to said bus (fig. 2a, ref. num 202);
- Receiving a digital content file for transmission across a distributed computer network (fig. 7, ref. num 702);
- Examining data comprising the digital content file, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network (fig. 7, ref. num 704 and 706).

Gupta et al. does not teach using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file

and **the** related digital signatures, the examining is to determine whether the digital content file comprises a restricted data format, transmitting the digital content file if the data comprising the digital content file does not include the restricted data format, and blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver.

Hale et al. teaches the examining is to determine whether the digital content file comprises a restricted data format (col. 3, lines 9-12), transmitting the digital content file if the data comprising the digital content file does not include the restricted data format and blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, **wherein the restricted data format is an MP3 data format, a MPEG video data format, and a Word document format** (col. 3, lines 12-17), wherein the blocking is effected prior to a transmission of the digital content file to a receiver (col. 3, lines 12-17).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine examining a content file for restricted data formats, and transmitting the content file if not restricted data formats exist & blocking transmitting of restricted data formats do exist, as taught by Hale et al., to the restricted data format

infrastructure/device/system of Gupta et al. It would have been obvious for such modifications because preventing multimedia from being streamed protects copyrights (see col. 3, lines 1-9 of Hale et al.).

The combination of Gupta et al. as modified by Hale et al. still does not teach using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and related digital signatures. Gibbs et al. teaches using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and **the** related digital signatures**, the record including the related digital signatures** (fig. 4, ref. num 432, col. 6, lines 17-26, and col. 7, lines 56-67).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a router configured to log digital signatures related to the content file, as taught by Gibbs et al., to the restricted data format infrastructure/device/system of Gupta et al./Hale et al. It would have been obvious for such modifications because the steps above keep track of the status information and other information about the creation and authentication of digital signatures (see col. 3, lines 63-66 of Gibbs et al.).

Regarding claims 13 and 26, the combination of Gupta et al. in view of Hale et al. teaches all the limitations of claims 7 and 21, respectively, above. However, the

combination of Gupta et al. as modified by Hale et al. does not teach the examining is performed by a plurality of cache engines within the distributed computer network.

Gibbs et al. teaches the examining is performed by a plurality of cache engines within the distributed computer network (fig. 4, ref. num 420 and col. 7, lines 13-28).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a plurality of cache engines to perform the examining within the distributed computer network, as taught by Gibbs et al., to the method/network device of Gupta et al./Hale et al. It would have been obvious for such modifications because the use of a plurality of cache engines to perform examining within the distributed computer network allows faster examining of data as it is passed over the distributed computer network (see col. 7, lines 15-25 of Gibbs et al.).

Regarding claim 23, the combination of Gupta et al. in view of Hale et al. teaches all the limitations of claim 21, above. However, the combination of Gupta et al. as modified by Hale et al. does not teach wherein the digital signature applied to the content file within the distributed computer network is logged **to maintain a record for the content file and the digital signature** when the content file is transmitted across the distributed computer network.

Gibbs et al. teaches wherein the digital signature applied to the content file within the distributed computer network is logged **to maintain a record for the content file and the digital signature** when the content file is transmitted across the distributed computer network (fig. 4, ref. num 432, col. 6, lines 17-26 col. 7, lines 56-67).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the step of logging the digital signature applied to the content file when the content file is distributed, as taught by Gibbs et al., to the network device of Gupta et al./Hale et al. It would have been obvious for such modifications because the step of logging the digital signature applied to the content file when the content file is distributed keeps track of the status information and other information about the creation and authentication of digital signatures (see col. 3, lines 63-66 of Gibbs et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH